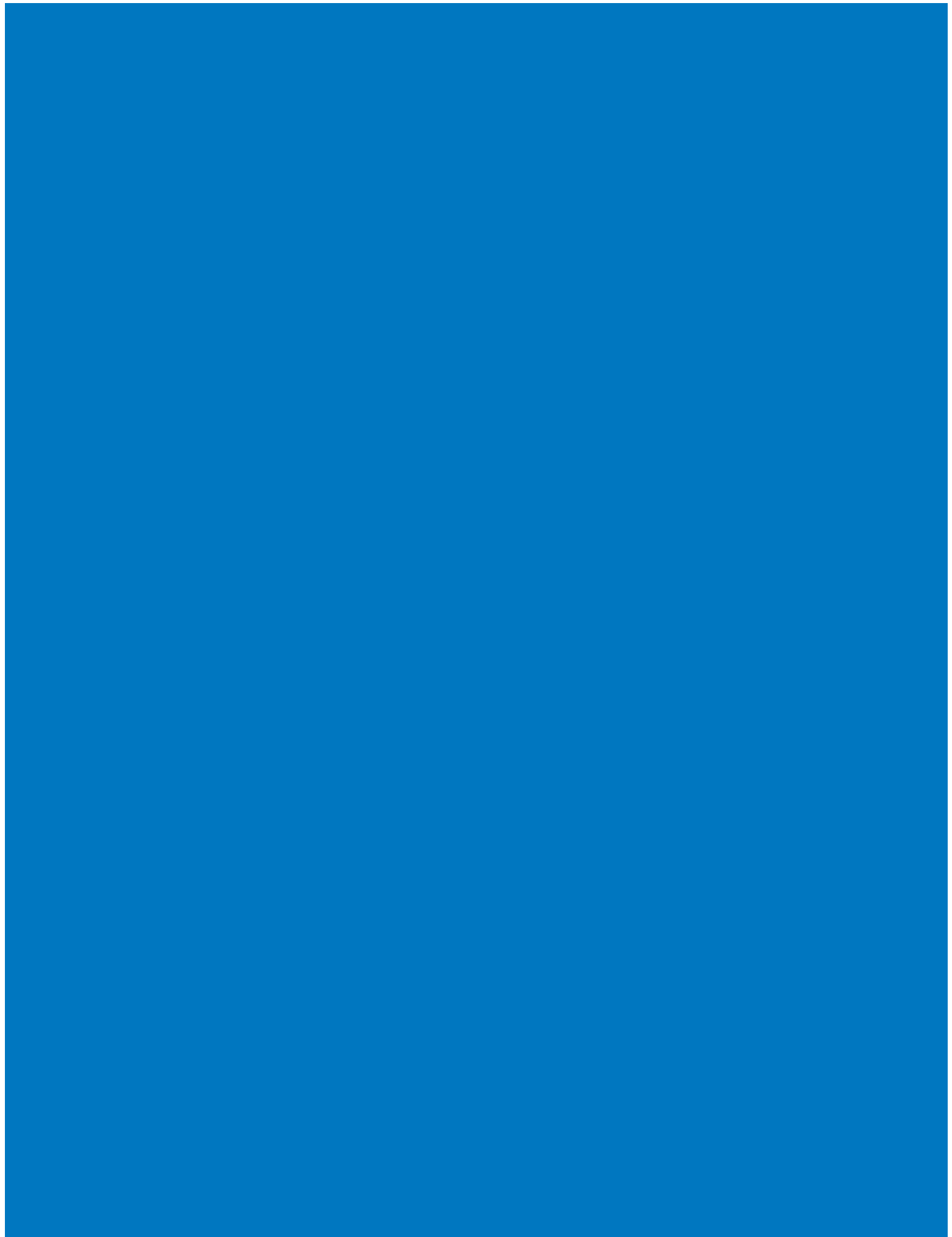


2012 Top Technology Initiatives Survey Results





Introduction

Securing the information technology environment is an increasingly complex challenge for public accounting firms, businesses and other organizations. The environment continues to evolve and change with advances in technology such as from hardware and ERP systems to virtualization and software as a service (SaaS). Organizations are increasing their use of information technology tools and other resources, adopting new technologies and exploring new ways to use technology.

As the use of information technology continues to grow and diversify, so do the risks in managing technology. So it is not entirely unexpected that securing the IT environment ranks first among the top ten information technology priorities for CPAs. The survey also found that leveraging emerging technologies is a growing issue for CPAs, both in the risks it presents and the opportunities it creates. The ranking is based on the 2012 Top Technology Initiative Survey of the American Institute of Certified Public Accountants (AICPA).

Survey respondents generally are confident about the ability of their organizations (or their clients' organizations) to meet their information technology goals for 2012 from information security to privacy to data management. However, CPAs are concerned about their organizations being able to avoid a data breach because of the loss of a smartphone, laptop, tablet or other mobile device. It is a concern that is widely shared.¹ CPAs also were not as confident in the ability of their organizations to leverage the benefits of emerging technologies such as mobile devices and cloud computing or to have the resources to support new revenue streams from these innovations.

"Whether you are a financial analyst or controller, internal controls auditor, external auditor, fraud investigator, or C-level executive," Janis Parthun, CPA, CITP, CGMA, Senior Technical Manager at the AICPA, suggests, "you are likely to be exposed to information technology if you interact with data."

Background to the Survey

The 2012 survey, conducted from Jan. 17-Feb. 15, was based on responses from 2,259 AICPA members who are interested in information technology. More than 40% are in public accounting firms, a third in business and industry, and the rest in other sectors such as consulting or government. Most of the respondents are at the manager or higher levels in their organizations. The survey was developed and managed by the AICPA's IT Division, part of Member Specialization and Credentialing.

This year, the survey employed a new methodology intended to explore IT issues in more depth. For the first time, participants were asked to rank the top technology priorities and their level of confidence in the ability of their organizations or their clients' organizations to address these priorities. As in last year's survey, they also were asked to rank the 2012 technology initiatives having the most impact on their organizations.

Proficiency in Information Technology

As the survey found, CPAs at every level of an organization are dealing with information technology as part of their day-to-day responsibilities – most of the survey respondents said they regularly or frequently encounter IT questions and concerns. Clients of public accounting firms and executives in corporations and businesses are looking to CPAs for advice and assistance in addressing a range of technology issues. For CPAs, the need to understand technology and to achieve proficiency in the use and management of information are growing in importance. Respondents indicated a desire to attain a higher level of proficiency in business intelligence as well as in risk management, fraud and information management. By contrast, CPAs generally are comfortable with their level of proficiency in the traditional areas of business reporting, audit/attest and internal controls.

¹ "Mobile devices expose organisations to unprecedented security risks, reports say," Jeff Drew, CGMA Magazine, Feb. 15, 2012. cgma.org/magazine/news/pages/20125134.aspx



Survey Findings

SURVEY RESULTS FIND THAT SECURING IT ENVIRONMENT IS TOP ISSUE FOR CPAS

The following is the ranking of the top ten information technology priorities for 2012. The figure in parentheses is the percentage of respondents who are either confident or highly confident their client or organization is achieving its goals.

- 1** Securing the IT environment (62 percent)
- 2** Managing and retaining data (61 percent)
- 3** Managing risk and compliance (65 percent)
- 4** Ensuring privacy (62 percent)
- 5** Leveraging emerging technologies (34 percent)
- 6** Managing system implementation (52 percent)
- 7** Enabling decision support and managing performance (46 percent)
- 8** Governing and managing IT investment/spending (56 percent)
- 9** Preventing and responding to fraud (60 percent)
- 10** Managing vendors and service providers (56 percent)

1 Securing the IT environment (information security)

The risks: An organization that has not considered all the vulnerabilities and threats related to information technology, and has an inadequate security policy, could be a serious risk. The loss, theft or compromise of a mobile device could disrupt an organization's operations and result in the loss of sensitive or confidential client and customer data. A cyber attack could have the same consequences. Cloud computing has many benefits, but complementary risks include ensuring that the vendor providing the cloud services is appropriately securing and managing the remote environment.

Risk management: Securing the IT environment begins with a risk assessment — an organization thoroughly considers its information technology vulnerabilities and threats. It then implements policies to mitigate those risks, including the safeguarding of networks and servers from cyber attack, securing all mobile devices including laptops, tablets and mobile phones from data breaches, and ensuring that data will be safe in the event of a cyber attack or mobile device loss. In addition, careful vendor due diligence and obtaining Service Organization Control (SOC) reports can help ensure that cloud computing risks are also identified and mitigated.

2 Managing and retaining data

The risks: An organization whose data management policies and procedures are insufficient or ineffective is exposed to the consequences of poor data management – for example, business decisions or client advice may be based on incomplete or inaccurate data. Another issue is storing data in outdated or incompatible formats for retrieval, or improperly backing up data, which can result in irrevocable loss of data.

Risk management: Managing and retaining data requires an organization to understand the internal, legal and compliance-related requirements for data retention and develop policies and procedures to satisfy those requirements. The organization has to

be able to back up its data and to restore data in the event of a data loss (or a need to access historical data). In addition, it must be able to manage the cost of storing and archiving data.

3 Managing risk and compliance

The risks: Organizations that do not understand and have not considered the risks associated with information technology are not prepared to mitigate those risks. As a result they may be especially vulnerable. By contrast, a sound risk management policy can help a company to reduce its risks. And companies with mature risk practices have stronger financial results, according to an Ernst & Young study.²

Risk management: In the past two years a number of companies have increased the time and resources devoted to risk management and CFOs are assuming more responsibility for risk management.³ To manage IT risk and compliance, an organization conducts a risk assessment, looking at vulnerabilities and threats including those related to emerging technologies like cloud computing, mobile technologies and social media. It then designs policies and internal controls to reduce IT-related risks to an acceptable level and it monitors the effectiveness of those controls. It also develops policies to detect management override abuse within IT-dependent systems. Finally, it ensures that it has adequately deployed automated controls to achieve separation of duties.

In managing risk and compliance, business enterprises must address a number of complex risks such as threats to cyber security and the safeguarding of information. In response, boards of directors and senior management of more organizations are adopting enterprise-wide policies and procedures for risk management. But not all organizations are on board. "Despite the growing trends towards adopting a broader top-down approach to risk oversight, not all organizations have taken steps to modify their procedures for identifying, assessing and managing risks, and in communicating risk information to key stakeholders, both internal and external to the organization," according to a report of the AICPA and North Carolina State University.⁴

² "Managing Risk for Better Performance," Ernst & Young.
ey.com/GL/en/Services/Advisory/Turning-risk-into-results-Managing-risk-for-better-performance

³ "Keeping Cool in the Hot Seat," Kate O'Sullivan, CFO.com, March 1, 2012.
www3.cfo.com/article/2012/3/risk-management_risk-management-cfo-concerns-cfo-role-responsibilities (see marker p. 6)

⁴ "Report on the Current State of Enterprise Risk Oversight: 3rd Edition," Research Conducted by the ERM Initiative at NC State on Behalf of the American Institute of CPAs Business, Industry & Government Team," August 2011.
aicpa.org/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/current_state_erm_3rdedition.pdf

4 Ensuring privacy

The risks: Privacy concerns the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information. A breach of privacy from data leaks from mobile technology, data breach in the organization, cyber attack or other causes could result in the unauthorized disclosure of personal information about employees, clients or customers and others.

Risk management: Most states have enacted privacy laws concerning the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information. Many impose significant and painful penalties for violations such as a breach in client data.⁵ To ensure privacy, CPAs in public accounting and business need to know the privacy laws of their home state as well as those of states or countries where their organizations and their clients and/or customers do business. Organizations establish privacy policies that address privacy laws and requirements, put privacy safeguards and controls in place, and secure data and systems to minimize the risk of a privacy breach. If there is a breach, an organization is prepared to quickly detect it and respond.

5 Leveraging emerging technologies

The risks: Smartphones, tablets, cloud computing and other emerging technologies have enabled CPAs to access, use and manage information most anywhere, anytime; and they and other users are taking full advantage. By 2015, more U.S. Internet users will access the Internet through mobile devices than through PCs or other wireline devices.⁶ But this unprecedented access to information has brought

new challenges for CPAs. Not only must CPAs understand and keep abreast of advancements in emerging technologies, they must also be prepared to assist their organizations to develop policies and procedures for their use, including security and privacy protections, and to identify and fund revenue opportunities and realize other benefits.

Risk management: Emerging technologies are driving change and innovation in markets, industries and organizations worldwide. The challenge for CPAs and their organizations is first to understand the risks in technologies that by definition are continuing to evolve. Organizations can then develop the plans, policies and systems to manage these risks, to train staff in the use of these technologies (or hire outside training providers), and access the financial resources and make decisions about how to capitalize on the revenue-generating opportunities in emerging technologies.

LEVERAGING EMERGING TECHNOLOGIES IS A GROWING CHALLENGE

To leverage emerging technologies, CPAs need to work with their IT counterparts (e.g., CIOs, IT Directors, IT consultants) to determine which emerging technologies can help to increase revenues, reduce costs, or otherwise improve the organization's ability to achieve its mission. Donny Shimamoto, CPA, CITP, CGMA, and chair of the AICPA's IT Executive Committee explains: "By partnering with IT, who will provide the technology expertise, CPAs can help their organizations build a good business case that balances the risk of emerging technologies with the potential benefits."

⁵ "Security Breach Laws and What a CPA Needs to Know About Privacy," James Bourke, CPA, CITP, CPA Insider, August 20, 2011. cpa2biz.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2011/CPA/Aug/SecurityBreach.jsp

⁶ "IDC: More Mobile Internet Users Than Wireline Users in the U.S. by 2015," IDC press release, 15 September 2011. idc.com/getdoc.jsp?containerId=prUS23028711

6 Managing system implementation

The risks: An organization's strategic goals drive its system implementation. If the goals and the implementation are not aligned, the organization may only partly meet its business goals for implementation – or not meet them at all. It may not realize its return on investment for an implementation project, and it may have other problems such as converting or transferring data inadequately.

Risk management: To manage system implementation, an organization establishes a strong alignment between its strategic goals and IT-related projects. In evaluating new projects, it considers the recommendations of internal advocates who know how to establish a strong business case for such projects. It analyzes and documents the business requirements for such projects, and it evaluates their value based on return on investment, earned value analysis and other criteria. Finally, it ensures the quality and integrity of project data.

7 Enabling decision support and managing performance

The risks: The reports provided to management should be aligned with an organization's strategic goals. However, this may not be the case if the organization's data architecture does not support an effective reporting system, or management has not supported an investment in business intelligence related projects. As a result, management may receive inaccurate or incomplete reports, and, consequently, may be at risk of making poorly informed business decisions.

Risk management: Enabling decision support and managing performance means that an organization maintains a strong alignment between its strategic goals and the reports provided to management. It has a management reporting environment and business intelligence infrastructure that supports effective decision-making. Its management has a good understanding of how data flow through the

organization and how those data support decision-making. Management uses reports that contain high-quality data — the data are accurate, complete, timely and auditable. Executives understand the technology options available to support business intelligence related initiatives, and they support the organization in implementing business intelligence and performance management initiatives.

8 Governing and managing IT investment and spending

The risks: If an organization does not have effective information technology governance policies and procedures, or an alignment between its IT and business strategies, it may not have a clear idea as to how to invest in information technology, or how to prioritize its spending. As a result, it may overspend or underspend on information technology initiatives, and not receive an adequate return on its investments in IT initiatives. Investment in IT “should provide benefits and synergies,” a survey respondent commented. “Too many disparate technologies, platforms and weak interconnections diminish the benefits of IT while raising costs.”

Risk management: An organization's ability to govern and manage IT investment and spending depends on it having a strong alignment between its mission/strategic plan and its IT strategy as well as a strong IT governance function. The organization is able to prioritize IT initiatives and related spending, manage its investment in such initiatives, and analyze the value of its IT investment portfolio. A risk-based approach can help organizations to invest wisely. According to a guide on IT security for CPAs, “the idea is to tabulate assets and holdings, assign them some value and then calculate the probability that a risk or threat might actually be realized in the form of a loss. It is prudent to take a risk-based approach when doing this, spending no more than the amount that might be lost, in order to reduce risk to an appropriate level.”⁷

⁷ “ABCs of IT Security for CPAs: A CPA's Introduction to IT Policies and Procedures,” Ed Tittel, AICPA. aicpa.org/interestareas/informationtechnology/resources/informationsecuritymanagement/downloadabledocuments/abcsecurity2_policyprocedure.pdf

9 Preventing and responding to fraud

The risks: Information technology has facilitated the perpetration of fraud in organizations. Those organizations that do not know how to identify IT-related fraud, do not have policies to prevent such fraud, and do not have plans to respond to a fraud, are particularly vulnerable. Likewise, organizations are at greater risk if they do not have policies to prevent management override opportunities within financial-related systems. If a fraud does occur, these organizations may not have plans in place to respond.

Risk management: To prevent and respond to fraud, an organization considers the fraud risks associated with information technology, designs policies and internal controls to mitigate such risks, and establishes policies to detect management override abuse. If a fraud is perpetrated, it is prepared to respond.

10 Managing vendors and service providers

The risks: Contracting with a vendor or service provider can save an organization time and money: the provider may have the knowledge and expertise to perform work more efficiently and at less cost than the company itself. But there are risks. The organization may not know how to seek the right service provider. It may not know how to negotiate a service level agreement (SLA), for example, it could find itself locked into an agreement without enough flexibility to adjust or exit the contract. The company may unknowingly take on the risks of the vendor, or it may come to distrust the vendor on issues of security or confidentiality or processing integrity; or it may find the vendor is not complying with terms of the SLA.

Risk management: An organization assesses the risk of using a provider, identifies reliable providers, performs the necessary due diligence before engaging a provider, and analyzes the costs of engaging a provider. It validates the sufficiency and completeness of the terms and conditions in a SLA and it knows whether the provider is in compliance with the SLA. The organization negotiates a flexible contract with the provider — if it chooses, it can reasonably adjust or exit the contract.

Impact of Technology Initiatives in 2012

- 1 Information security — securing the IT environment
- 2 Remote access
- 3 Control and use of mobile devices
- 4 Business process improvement with technology
- 5 Data retention policies and structure
- 6 Privacy policies and compliance
- 7 Staff and management training
- 8 Spreadsheet management
- 9 Overall data proliferation and control
- 10 Portals — vendor and client/customer

While the top three initiatives in 2012 were 1) information security, 2) remote access and 3) control and use of mobile devices, the top three in 2011 were 1) control and use of mobile devices, 2) information security and 3) data retention policies and structure. What this comparison shows is that information security and control and use of mobile devices remain among the top concerns of CPAs. This year, remote access replaced data retention policies in the top three, which may not be surprising, given CPAs' continuing concerns about remote access issues such as cloud computing.



INFORMATION TECHNOLOGY INITIATIVES

As in 2011, this year's survey asked respondents to list the top ten information technology initiatives that are having the most impact on their organizations.

Public Accounting and Business and Industry Perspective

The responses of CPAs in public accounting and in business and industry were analyzed to provide another perspective on the survey results.

The following are the top ten technology priorities from the perspective of those in public accounting and those in business.

Public Accounting Perspective		Business and Industry Perspective	
1.	Securing the IT Environment	1.	Securing the IT Environment
2.	Managing and Retaining Data	2.	Managing Risk & Compliance
3.	Ensuring Privacy	3.	Managing and Retaining Data
4.	Managing Risk & Compliance	4.	Managing System Implementations
5.	Leveraging Emerging Technologies	5.	Enabling Decision Support and Managing Performance
6.	Preventing & Responding to Fraud	6.	Leveraging Emerging Technologies
7.	Governing & Managing IT Investment & Spending	7.	Governing & Managing IT Investment & Spending
8.	Managing System Implementation	8.	Managing Vendors & Service Providers
9.	Enabling Decision Support and Managing Performance	9.	Ensuring Privacy
10.	Understanding IT Impacts of Legislation, Regulations and Standards	10.	Preventing and Responding to Fraud

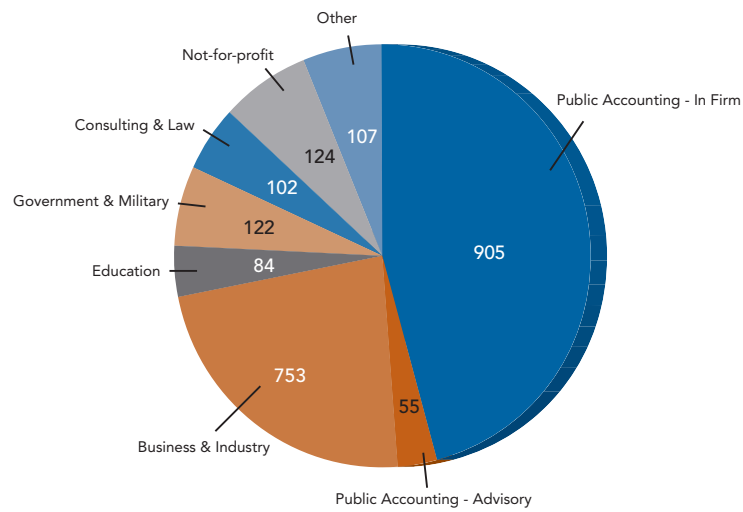
As with the overall survey responses, those from CPAs in public accounting ranked securing the IT environment as the No. 1 goal for their organizations in 2012. The other priorities of CPAs in public accounting and business matched the overall priorities, except that public accounting CPAs included understanding the IT impacts of legislation, regulation and standards on their top ten (in lieu of managing vendors & service providers). While the priorities were nearly the same, the rankings differed somewhat. For example, managing system implementation ranked No. 8 on the public accounting list but No. 4 on the business and industry list.

In summary, CPAs generally are confident of the ability of their organizations (or their clients' organizations) to meet their top technology goals for 2012. Their main concerns are whether their organizations can avoid data compromises from losses of mobile devices. They also are concerned about the ability of their organizations to leverage the benefits of emerging technologies. CPAs can address these concerns by assisting their organizations to address the risks in the increasing use of mobile technology and to capitalize on the benefits that emerging technologies have to offer.

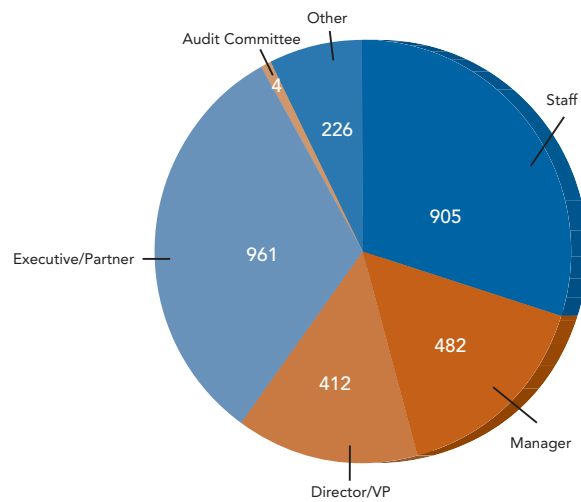
Appendix

This appendix contains the second-tier details to the confidence levels associated with the top five 2012 Top Technology Priorities. This information includes combined summary results for public accounting and business and industry. Not all the data results are presented here. To learn more or to access the comprehensive results, visit aicpa.org/toptech.

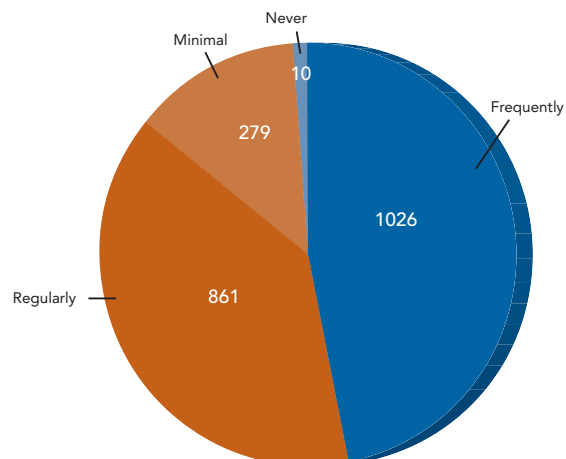
Which Industry do you work in?



What is your job responsibility in your firm or organization?



How often do you encounter information technology questions or concerns in your field of work?



The 2012 Top 10 Technology Priorities

What are the top five priorities for your client or organization in 2012?

Ranking	Priority	Respondent Count	Percentage of Total Respondents
1	Securing the IT environment	1,442	64%
2	Managing & retaining data	1,349	60%
3	Managing risk & compliance	1,279	57%
4	Ensuring privacy	1,047	46%
5	Leveraging emerging technologies	1,033	46%
6	Managing system implementations	948	42%
7	Enabling decision support & managing performance	927	41%
8	Governing and managing our IT Investment/ Spend	925	41%
9	Preventing & responding to fraud	792	35%
10	Managing vendors & service providers	621	27%
11	Understanding IT impacts of legislation, regulations and standards	454	20%
12	Using service organizations and SOC Reports	91	4%
13	Other	68	3%

Confidence Level of the Top Priorities

How confident are you that your client or organization is appropriately:

Ranking	Topic	Confidence Index	Percentage of Respondents Who are Confident or Highly Confident
1	Using service organizations and SOC Reports	3.09	30%
2	Leveraging emerging technologies	3.11	34%
3	Understanding IT impacts of legislation, regulations and standards	3.23	40%
4	Enabling decision support & managing performance	3.34	46%
5	Managing system implementations	3.45	52%
6	Governing and managing our IT investment/spend	3.55	56%
7	Managing vendors & service providers	3.55	56%
8	Preventing & responding to fraud	3.60	60%
9	Managing & retaining data	3.61	61%
10	Securing the IT environment	3.65	62%
11	Ensuring privacy	3.66	62%
12	Managing risk & compliance	3.68	65%

Ranking is from LEAST confident to the MOST Confident (5.0).

No. 1 - Securing the IT Environment

Please indicate your agreement with the following statements based on the following scale - I am confident that my client or organization:

Ranking	Factor to Consider	Confidence Index	Percentage of Respondents Who are Confident or Highly Confident
1	Has properly protected all mobile devices to prevent a data breach	3.20	41%
2	Will be safe in the event of a cyber attack or mobile device loss	3.22	40%
3	Has considered all of the relevant vulnerabilities and threats pertaining to IT	3.39	50%
4	Has a security policy that addresses information security risks appropriate to our size of organization and industry	3.57	59%
5	Has properly protected our network/servers from cyber-attack	3.69	63%

Ranking is from LEAST confident to the MOST Confident (5.0).

No. 2 - Managing & Retaining Data

Please indicate your agreement with the following statements based on the following scale - I am confident that my client or organization:

Ranking	Factor to Consider	Confidence Index	Percentage of Respondents Who are Confident or Highly Confident
1	Is adequately managing the cost of storing and archiving data	3.68	61%
2	Has appropriately designed data retention policies and procedures to meet our data retention requirements	3.71	66%
3	Understands data retention requirements (internal, legal and compliance-related)	3.86	74%
4	Is properly backing up its data and will be able to restore data in the event of an operational data loss or need to access historical data	4.02	78%

Ranking is from LEAST confident to the MOST Confident (5.0).

No. 3 - Managing Risk and Compliance

Please indicate your agreement with the following statements based on the following scale - I am confident that my client or organization:

Ranking	Factor to Consider	Confidence Index	Percentage of Respondents Who are Confident or Highly Confident
1	Has considered all of the relevant vulnerabilities and threats pertaining to IT, including those related to emerging technologies like cloud computing, mobile technologies, and social media	3.36	48%
2	Has appropriate policies in place to detect management override abuse within IT-dependent systems	3.37	47%
3	Is effectively monitoring the effectiveness of our IT-related internal controls	3.39	48%
4	Has been able to adequately deploy automated controls to achieve separation of duties	3.39	49%
5	Has conducted an IT risk assessment appropriate to the level of complexity of our IT environment	3.45	52%
6	Has appropriately designed our policies and internal controls to reduce our IT-related risks to an appropriate level	3.53	56%
7	Has a good understanding of the appropriate regulatory and compliance requirements related to IT for our size of organization and industry	3.54	56%
8	Understands the risks associated with Information Technology (IT)	3.86	73%

Ranking is from LEAST confident to the MOST Confident (5.0).

No. 4 - Ensuring Privacy (Confidence Factor)

Please indicate your agreement with the following statements based on the following scale - I am confident that my client or organization:			
Ranking	Factor to Consider	Confidence Index	Percentage of Respondents Who are Confident or Highly Confident
1	Will be able to quickly detect and respond to a privacy breach incident	3.42	47%
2	Has put the appropriate privacy safeguards and controls in place to minimize our risk of a privacy breach	3.68	63%
3	Has appropriately secured our data/systems to minimize our risk of a privacy breach	3.70	63%
4	Has a good understanding of the appropriate regulatory and compliance requirements related to privacy of data for our size of organization and industry	3.73	65%
5	Has a privacy policy that addresses the requirements and risks appropriate to our size of organization and industry	3.74	65%

Ranking is from LEAST confident to the MOST Confident (5.0).

No. 4 - Ensuring Privacy (Concern Factor)

Please indicate your agreement with the following statements based on the following scale - I am concerned that:		
Ranking	Factor to Consider	Confidence Index
1	There is an increasing need for organizations to protect PII (personally identifiable information) due to use of location-based services	3.89
2	Private data will be disclosed in the event of a data breach in our organization	3.50
3	There are stricter regulatory enforcements – by state, federal, and government and internationally related to Privacy	3.48
4	Private data will be disclosed in the event of a breach in the cloud computing environment	3.46

Ranking is from MOST confident to the LEAST Confident (5.0).

No. 5 - Leveraging Emerging Technologies

Please indicate your agreement with the following statements based on the following scale - I am confident that my client or organization:

Ranking	Factor to Consider	Confidence Index	Percentage of Respondents Who are Confident or Highly Confident
1	Has the appropriate staff and resources to support new revenue opportunities related to IT	2.93	27%
2	Has the necessary knowledge to identify on new revenue opportunities related to IT	3.19	36%
3	Understands and is appropriately managing the risk associated with emerging technologies	3.29	43%
4	Has access to resources (e.g., training, consultants, internal staff/ knowledge) to enable staff to leverage new technologies	3.39	51%
5	Has the financial resources (e.g., capital/credit) to support adoption of emerging technologies	3.46	54%

Ranking is from LEAST confident to the MOST Confident (5.0).

Impact of Technology Initiatives in 2012

Please identify the level of impact of the following technology initiatives on your organization and its key constituents for 2012.

Ranking	Priority	Impact Index
1	Information security	3.47
2	Remote access	3.39
3	Control and use of mobile devices	3.35
4	Business process improvement with technology	3.26
5	Data retention policies and structure	3.26
6	Privacy policies and compliance	3.26
7	Staff and management training	3.25
8	Spreadsheet management	3.08
9	Overall data proliferation and control	3.06
10	Portals (vendor and client/customer)	3.05

Note: Similar to 2011, this year's survey asked respondents to list the top ten information technology initiatives that are having the most impact on their organizations.



888.777.7077 | ITinfo@aicpa.org | aicpa.org/infotech